# NORTH DAKOTA

# HOMELAND SECURITY

# ANTI-TERRORISM SUMMARY

**The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.**

## NDSLIC Disclaimer



## QUICK LINKS

# North Dakota

**Over 1,000 acres burned in Mandaree wildfire.** A wildfire has burned more than 1,000 acres near Mandaree, North Dakota, KFYR 5 Bismarck reported September 20. According to a Three Affiliated Tribes Fire Management officer, crews arrived September 19 to a wildfire created by warm temperatures and strong winds. As of September 20, the fire was 35 percent contained. No structures were burned. Source: http://www.kfyrtv.com/News_Stories.asp?news=59368

**ND stiffens rules for female cattle imports.** North Dakota stiffened cattle import rules because of cases of a bovine venereal disease in other States, the Associated Press reported September 18. The State veterinarian said the board of animal health recently voted to tighten the restrictions for female cattle imports because of concerns about trichomoniasis, which can cause infertility and miscarriages in cattle. She said officials expect more cattle to be brought into North Dakota because of drought in other States. Source: http://www.necn.com/09/18/12/ND-stiffens-rules-for-female-cattle-impo/landing_nation.html?&apID=b6906ccb2686452cacb683a2a1be0109

**Bomb threat evacuates downtown Fargo Hotel.** A bomb threat evacuated the downtown Radisson Hotel in Fargo, North Dakota, for nearly 2 hours September 15, the region's fourth such threat in a week. A Fargo police lieutenant said the threat was made in a phone call to Radisson staff, at which point the hotel made the decision to evacuate guests. After police officers arrived and performed a cursory search of the building it was determined there was no validity to the threats made in the call. Hotel guests were allowed back into the building after the police cleared the scene. The incident followed similar threats to the Fargo Hector International Airport September 11, the Grand Forks International Airport September 12, and North Dakota State University September 14. The police are treating September 15's threat as separate, but are not ruling out the possibility that it is related to the others made over the week. Source: http://www.jamestownsun.com/event/article/id/169425/group/News/

# Regional

(South Dakota) **South Dakota ag officials advise tests for aflatoxin levels in corn.** South Dakota agriculture officials advised farmers and ranchers to test for aflatoxin levels in their corn, distiller's grains, and silage piles due to the 2012 drought, the Associated Press reported September 20. South Dakota State University Extension educators said feed refusal, reduced growth rate, and decreased feed efficiency are the predominant signs of chronic aflatoxin poisoning in livestock. High levels of aflatoxin fed to dairy cows can lead to contamination of the milk that is produced. The National Corn Growers Association said aflatoxin is most prevalent in corn, cotton, peanuts and tree nuts. Source: http://www.ksfy.com/story/19592742/south-dakota-ag-officials-advise-tests-for-aflatoxin-levels

# National

**USDA expands drought assistance to 22 states.** September 20, the U.S. Secretary of Agriculture announced an additional $11.8 million in financial and technical assistance to help crop and livestock producers in 22 States apply conservation practices that reduce the impacts of drought and improve soil health and productivity. The announcement expanded upon previous efforts and brought the total assistance to nearly $28 million. Funding targeted States that are experiencing either exceptional or extreme drought conditions. Exceptional drought continues to dominate sections of Arkansas, Colorado, Georgia, Iowa, Kansas, Kentucky, Missouri, Nebraska, New Mexico, Oklahoma, South Dakota, Tennessee, Texas, and Wyoming. Source: http://www.agprofessional.com/news/USDA-expands-drought-assistance-to-22-states-170339366.html

# International

**Turkey security forces seize radioactive material, Anatolia says.** Turkey's paramilitary police seized radioactive materials with an estimated market value of $1.3 million, the Anatolia news agency said September 18. The state-run agency said two tubes of cesium-137, a highly poisonous radioactive chemical, were seized near the northern town of Espiye in Giresun province. Source: http://www.businessweek.com/news/2012-09-18/turkey-security-forces-seize-radioactive-material-anatolia-says

**26 killed in Mexico pipeline fire near US border.** A fire that erupted at a natural gas pipeline distribution center near Mexico's border with the United States has killed 26 people, the Associated Press reported September 19. Mexico's state-owned oil company, Petroleos Mexicanos, initially reported 10 deaths at the facility near the city of Reynosa, across from McAllen, Texas. Later, the death toll was raised to 26 maintenance workers. One man killed was run over when he rushed onto a highway running away from the facility. The fire also forced evacuations of people in nearby ranches and homes. The company said later that the blaze was extinguished in 90 minutes and the pipeline was shut off. Forty-six workers were injured. Source: http://www.necn.com/09/19/12/26-killed-in-Mexico-pipeline-fire-near-U/landing_nation.html?&apID=6cc908fdd0774468b1a7f3dfcb1674a0

**Foreign journalists in China targeted by malware attacks.** Foreign journalists in Beijing, China, have been targeted by two very similar malware attacks in just over 2 weeks in the lead-up to China's once-in-a-decade leadership transition. The emails, one appearing to come from a Beijing-based foreign correspondent and the other from a Washington-based think tank, both contained an attachment with the same type of malware, according to an independent cyber security expert who reviewed the files. A government spokesman warned against jumping to conclusions about who was responsible. Both of the emails referred to the upcoming handover of power in the top ranks of the ruling Communist Party. The attachment, if opened, would have installed malware that sent encrypted information from the user's computer to an external server. That server is hosted in England. Source: http://www.reuters.com/article/2012/09/14/us-china-malware-idUSBRE88D0CU20120914

**French police reinforce security around US Embassy.** Police said they are reinforcing security around the American Embassy in Paris, France, after hundreds of people gathered outside the building September 15 to protest a film produced in the United States that insults the Prophet Muhammad. A police officer said more uniformed and plain clothes police were put in place September 16 on the streets surrounding the embassy. He said that 150 people were detained September 15 and had their ID's checked because the protest was unauthorized. One person remained in custody for roughing up an officer. The demonstration was part of a wave of protests outside U.S. diplomatic posts around the world, some of which have turned violent. Source: http://www.cbsnews.com/8301-501714_162-57513733/french-police-reinforce-security-around-us-embassy/

**Al Qaeda branch in North Africa calls for attacks on US diplomats.** Al Qa'ida's branch in North Africa is calling for attacks on U.S. diplomats and an escalation of protests against an anti-Islam video that triggered a wave of demonstrations in Muslim countries. In a statement released September 18, al Qa'ida in the Land of the Islamic Maghreb praised the killing of the U.S. ambassador to Libya, in an attack on the U.S. consulate in Benghazi September 11. The group threatened attacks in Algeria, Tunisia, Morocco, and Mauritania in response to the movie that denigrates the Prophet Muhammad. Yemen-based al Qa'ida in the Arabian Peninsula recently issued a similar call for attacks on U.S. diplomatic facilities. The group is al Qa'ida's most active branch in the Middle East. Source: http://www.foxnews.com/world/2012/09/18/al-qaeda-branch-in-north-africa-calls-for-attacks-on-us-diplomats/

**Violence over anti-Islam film in 3 nations.** Demonstrations against an anti-Islam film turned violent the weekend of September 14 outside a U.S. Consulate in Karachi, Pakistan, the U.S. Embassy in Jakarta, Indonesia, and a U.S. military base in Afghanistan. Hundreds of protesters clashed with police when they tried to storm the U.S. Consulate in Karachi. One protester was killed and more than a dozen were wounded. In Jakarta, hundreds of Indonesians angered over the film clashed with police outside the U.S. Embassy, hurling rocks and firebombs and setting tires alight outside the mission. At least 10 police were rushed to the hospital after being pelted with rocks and attacked with bamboo sticks, said Jakarta's police chief. He said four protesters were arrested and one was hospitalized. Demonstrators burned a picture of the U.S. President and also tried to ignite a fire truck parked outside the embassy after ripping a water hose off the vehicle and torching it, sending plumes of black smoke billowing into the sky. Police used a bullhorn to appeal for calm and deployed water cannons and tear gas to try to disperse the crowd. In the central Java town of Solo, protesters stormed KFC and McDonald's restaurants, forcing customers to leave and management to close the stores. Source: http://www.navytimes.com/news/2012/09/ap-afghan-protest-over-anti-islam-film-turns-violent-091712/

## Banking and Finance Industry

**Bank of America website slows; Prophet film threat made.** Bank of America Corp's online banking Web site suffered intermittent problems September 18 amid threats on the Internet

that a group was planning to launch cyber attacks on the bank and other U.S. targets to protest a film that stirred unrest in the Middle East. Someone claiming to represent —cyber fighters of Izz ad-din Al qassam  said it would attack the Bank of America and the New York Stock Exchange in a statement posted on pastebin.com. Bank of America said its Web site was available but some customers might experience occasional slowness. The New York Stock Exchange declined to comment. Bank of America customers reached by Reuters in New York, Georgia, Ohio, and Michigan said they could not access the Web site. Source: http://news.yahoo.com/customers-reporting-bofa-website-problems-183410329--sector.html

**Bogus 'Refund Pending' emails targeting PayPal customers.** Fake PayPal notifications about a bogus refund are hitting inboxes around the world, trying to trick users into following the offered link and supposedly log into their accounts to receive it. The link will take users to a page that looks like PayPal's log-in page, but is actually a fake one mimicking PayPal's, and all the information submitted gets forwarded directly to the phishers behind the scheme. 1They will then likely use it to hijack the victim's PayPal and gain entrance to other online accounts. Source: http://www.net-security.org/secworld.php?id=13615

**'How I crashed my bank, stole PINs with a touch-tone phone'.** Miscreants can crash or infiltrate banks and help desks' touch-tone and voice-controlled phone systems with a single call, a security researcher warned, according to The Register September 18. A researcher who works for iSight Partners said audio processing algorithms in office telephone networks and speech-driven command software are liable to crash when bombarded with unusual data in —fuzzing  attacks. Certain DTMF (Dual-Tone Multi-Frequency) signals can cause private branch exchanges (PBX) and interactive voice response (IVR) systems to raise exceptions and bail out, much in the same way unexpected input data can disrupt applications running on a desktop computer or server. PBX and IVR machines are often used to run phone banking, call centers, and other interactive telephone systems. Given the appropriate DTMF input, it may be possible to crash backend application servers or convince them to cough up sensitive data. Repeating the trick to bring down a machine effectively launches a denial-of-service attack on the phone line as a paper by the researcher explained. —We would be able to extract sensitive information about the application's hosted environment with these sorts of bugs. Since applications that use DTMF algorithms are mainly phone-based, it was possible to extract output in the form of audio data , he said. He also claimed it was possible to extract customer PINs from an unnamed Indian bank. Source: http://www.theregister.co.uk/2012/09/18/dtmf_phone_system_hack_attack/

**FBI: Networks of financial institutions targeted with malware, RATs, and keyloggers.** A FBI report shows that cybercriminals have started focusing their efforts on targeting the networks of financial institutions, Softpedia reported September 18. Cybercriminals are relying on spam, keyloggers, Remote Access Trojans (RATs), phishing, and other malicious elements to steal employee log-in credentials. The Internet Crime Complaint Center (IC3) reported that the stolen information has been utilized to perform unauthorized wire transfers for amounts between $400,000 and $900,000. In the first phase of these operations, the criminals use spam and phishing emails. Once they compromise the machine of an employee, they plant RATs,

keyloggers, and other pieces of malware to gain access to internal networks and the details needed to access third party systems. Most of the victims appear to be small to medium-sized banks and credit unions, but major financial institutions have also been targeted. In some cases, the crooks launched distributed denial-of-service attacks against the bank's Web site, most likely to cover up their fraudulent transactions. Source: http://news.softpedia.com/news/FBI-Networks-of-Financial-Institutions-Targeted-with-Malware-RATs-and-Keyloggers-293126.shtml

(Mississippi) **Woman says men strapped bomb to her, told her to rob bank.** A woman told police that she was forced to strap on a backpack she thought contained explosives and was told to rob a Canton, Mississippi bank, the Associated Press reported September 14. The woman walked into a Trustmark bank and told employees she had a bomb and they should call police, the Canton police chief said. She told police that two men attacked and kidnapped her near a gas station in Canton. The men threatened to kill the woman and hurt her child if she did not rob the bank, the police chief said. She told police the men told her to keep the bank doors open so they could watch her during the robbery. Police closed down some of the streets in the area for several hours and told residents they were to stay inside with their doors locked. FBI officials said it had not been determined if the device was an actual bomb. The backpack was safely detonated by bomb squad members. Source: http://www.wapt.com/news/central-mississippi/Police-Men-strapped-bomb-to-woman-told-her-to-rob-bank/-/9156946/16604466/-/r8nyof/-/index.html

## Chemical and Hazardous Materials Sector

Nothing Significant to Report

## Commercial Facilities

(Kansas) **Copper thieves cause $750,000 in damage.** Copper thieves tore out electrical systems at the Kamen Industrial Park in Wichita, Kansas, causing about $750,000 in damage, the Associated Press reported September 17. Police said the vandals stole about 2,000 feet of copper wiring. The thieves hit the roof of the building tearing out electrical systems to get to the copper wiring. Source: http://www.salina.com/news/story/copper-thefts-9-17-12

## Communications Sector

**T-Mobile USA, RIM resolve issue that hurt some BlackBerry users.** Research In Motion Ltd said September 18 a service disruption that affected Internet browsing for some BlackBerry users on T-Mobile USA's network had been resolved. T-Mobile September 18 said some of its BlackBerry smartphone users were unable to use the device for emails or Internet browsing. The partial service disruption was limited to customers of the BlackBerry 9900 and did not affect phone call services and text messaging, according to T-Mobile USA, a unit of Deutsche Telekom. Source: http://www.chicagotribune.com/business/sns-rt-us-researchinmotion-tmobileusabre88h18x-20120918,0,4103378.story

**Hacked touch tones crash phone networks, steal data.** According to one security researcher, interactive voice response systems (IVRs) — the ones people use to check and store voicemail and the ones people interact with when they call the bank — are so insecure that they could be tricked into spitting out sensitive information or taken down completely with just a single phone call. —No banks or organizations are testing IVRs because they think the systems are secure, but in reality, they are not. No firewall or CAPTCHAs monitor voice traffic, said a spokesman who works for security company iSight Partners. He explained that when a system's audio processing algorithms are fed strange DTMF (dual-tone multi-frequency) signals, it can cause the entire system to behave strangely or crash calls. Source: http://www.securitynewsdaily.com/2289-phone-hack-data-dump.html

**Developer warns millions of Virgin Mobile subscribers about authentication flaw.** An Alamo, Texas developer September 17 warned Virgin Mobile U.S. subscribers that their accounts can be hacked after the company failed to respond with a fix. —I reported the issue to Virgin Mobile a month ago and they have not taken any action, nor informed me of any concrete steps to fix the problem, so I am disclosing this issue publicly, he said in a blog post. He said he found that the carrier's current authentication method relied on the user's phone number and a six-number PIN to access an account. Using his own account, he created a script to narrow in on the 1 million possible passwords. Once the script unlocked his numeric PIN he realized —pretty much anyone can log into your Virgin Mobile account and wreak havoc, as long as they know your phone number. He said he contacted the firm and its parent, Sprint, in August to alert them to the issue but became frustrated with the pace of the investigation and lack of communication. After several emails back and forth with a Sprint official, he was told September 14 the company did not plan further action on Virgin Mobile's end. Source: http://threatpost.com/en_us/blogs/developer-warns-millions-virgin-mobile-subscribers-about-authentication-flaw-091712

(South Carolina) **Damage costly as highwire copper thieves disrupt cable service.** Authorities in South Carolina are looking for the copper thief or thieves who —somehow reached the cable/phone lines measuring from one telephone pole to another (which is approximately 400 feet and approximately 35 feet from ground), cutting them, stealing the copper wiring, fibrotic cables and metal conduit lines, according to a Spartanburg County sheriff's report. Neighbors reported loss of service beginning September 14. The theft in Chesnee involved equipment belonging to Chesnee Communications and Charter Communications, and will result in roughly $10,000 in repairs for each company, a sheriff's deputy said. Source: http://www.greenvilleonline.com/article/20120915/NEWS/309150111/Damage-costly-highwire-copper-thieves-disrupt-cable-service?odyssey=tab|topnews|text|FRONTPAGE&gcheck=1&nclick_check=1

## CRITICAL MANUFACTURING

**Feds expand Hyundai Elantra air bag probe after severed ear claim.** The National Highway Traffic Safety Administration added the 2011 and 2013 model years to an investigation of an air bag problem with 2012 Hyundai Elantras that cut a car owner's ear in half, the Associated Press

reported September 17. The agency also upgraded the probe to an engineering analysis, a step closer to a recall. The agency started investigating 123,000 2012 Elantras in May, but now said only Korean-built Elantras have the part that caused the problem. About 75,000 were sold in the U.S. In April, an Elantra owner told investigators a side air bag inflated in a crash and a metal bracket sliced the driver's ear. Hyundai said the problem appears to be isolated. Source: http://www.freep.com/article/20120917/BUSINESS01/120917049/Feds-expand-Hyundai-Elantra-air-bag-probe

**Got a BMW? Thicko thieves can easily nick it with $30 box.** BMWs and other high-end cars are being stolen by unskilled criminals using a $30 tool developed by hackers to defeat the on-board security systems, The Register reported September 17. The new tool is capable of reprogramming a blank key, and allows non-technical car thieves to steal a vehicle within 2 or 3 minutes or less. On-board diagnostics (OBD) bypass tools are being shipped from China and Eastern Europe in kit form with instructions and blank keys, said a news report linking the release of the tool to a spike in car thefts in Australia, Europe, and elsewhere during 2012. Would-be car thieves need to grab the transmission between a valid key fob and a car before reprogramming a blank key, which can then be used to either open the car or start it, via the OBD system. —Crooks only need to monitor a person using the key or interrogate the key fob to get enough information to decipher the key, explained a professor from the center for cyber security sciences at London's City University. Weak cryptography combined with a —security through obscurity approach on the OBD specification allows the tactic to succeed. A post from Pistonheads suggests that devices similar to those used in BMWs are also available for Opel, Renault, Mercedes, Volkswagen, and Toyota cars. Source: http://www.theregister.co.uk/2012/09/17/bmw_car_theft_hack/

## Defense/ Industry Base Sector

**Internet Explorer zero-day targeting defense industry.** Researchers at AlienVault discovered new versions of the new zero-day vulnerability in Internet Explorer that are targeting a number of defense and industrial companies, including a U.S. aircraft and weapons delivery systems firm, a U.S. aerospace and defense technology company, and a U.K. defense contractor. —We also found a fake domain of a company that builds turbines and power sources used in several applications including utilities and power plants, a researcher said. —We were able to check that the official Web site of the company has been compromised as well and it is serving the Internet Explorer ZeroDay to the visitors. They've included an iframe to the exploit in the entry page. The researcher and his team also found the exploit code evolved and is now able to infect not only Windows XP but also Windows 7 32-bit running Java 6. Source: http://www.infosecurity-magazine.com/view/28357/

**NNSA expands nuclear arms data collection, auditors say.** The U.S. National Nuclear Security Administration (NNSA) expanded its collection of information for identifying physical problems in the nation's nuclear weapons, the Energy Department's inspector general concluded in a new report. Steps have been taken to address —gaps in stockpile surveillance information that the semiautonomous Energy Department branch identified 2 years ago as obstacles to an

initiative to step up the pace of oversight efforts, according to the assessment. The agency increased its collection of such data by —increasing funding and expanding laboratory tests, the paper states. The heads of U.S. nuclear weapons laboratories —expressed concerns in their annual assessments about gaps of surveillance data due to a reduction in laboratory tests, the document says. The atomic agency in fiscal 2011 —increased surveillance funding within the Directed Stockpile Work program by $58 million, auditors wrote. The move allowed for a —142 percent increase (from 24 to 58 tests) in laboratory tests, as well as other oversight changes, according to the report. —NNSA plans to continue funding the surveillance program at or above the [fiscal year] 2011 level for future years, it adds. —According to a senior NNSA official, the laboratory directors assured NNSA that the proposed out-year funding will be sufficient to perform surveillance activities to affirm confidence in the stockpile. Source: http://www.nti.org/gsn/article/us-expands-nuclear-arms-data-collection-auditors/

## Emergency Services

(Idaho) **Volunteer firefighter charged with starting destructive wildfire.** A volunteer firefighter with the Clear Creek Fire Department was accused of intentionally starting a wildfire that has charred 250 acres and destroyed one home near the Robie Creek area, KTVB 7 Boise reported September 18. Sheriff's deputies arrested the man September 17 as he was actively fighting the Karney Fire. It was said that he confessed to starting the fire during questioning. He is now in the Ada County Jail. The Boise County Sheriff's Office reports the Karney Fire started September 17, and grew overnight. By September 18, the fire continued to grow after jumping a fire line and burning close to two homes in the Robie Creek area, but firefighters managed to keep those homes safe. The flames were threatening around 100 homes near the Robie Creek and Wilderness Ranch communities northeast of Boise. Officials said 80 homes in the area have been evacuated. The Karney Fire is only 15 percent contained at this point. The Red Cross set up an aid station at the Idaho City High School. Source: http://www.ktvb.com/news/Suspect-accused-of-starting-Wilderness-Ranch-wildfire-170186686.html

(California) **Sixteen fire hydrants stolen in northwest Redlands, estimate $40,000 to replace.** The city of Redlands, California, September 17 announced the theft of 16 fire hydrants in northwest Redlands. The estimated cost of replacing the missing hydrants is $40,000, according to Redlands Municipal Utilities and Engineering Department staff. The thefts occurred between September 11-12. Source: http://redlands.patch.com/articles/sixteen-fire-hydrants-stolen-in-northwest-redlands-est-40-000-to-replace

(Florida) **Undercover cops use smartphones to monitor protests.** A network that allowed undercover police to use smartphones and tablets to monitor and communicate during protests at the Republican National Convention has given new meaning to having —eyes on the ground, National Journal reported September 17. At the 2012 Republican National Convention in Tampa, Florida, police tried out a new tool that can turn officers' smartphones into multimedia surveillance and communication platforms. In Tampa, emergency responders used specialized apps and software to turn off-the-shelf smartphones and tablets into tools for sending real-time video, voice, and data. That allowed undercover officers to transmit real-time video, for example, of protesters

as they moved about the streets. The network in Tampa was used with special permission from the Federal Communications Commission. It was part of an effort to eventually develop a similar $7 billion National Public Safety Broadband Network for everyday use across the country. In addition to law-enforcement surveillance and communication, a future network could allow firefighters to transmit building plans to each other, or allow paramedics to review multimedia health records. Source: http://mashable.com/2012/09/17/smartphones-monitor-protests/

**Safety regulators looking at Ford police cars.** Government safety regulators are investigating Ford's Crown Victoria police cars due to complaints about defective steering columns, the Associated Press reported September 15. The probe affects about 195,000 cars from the 2005 through 2008 model years. The government has received three complaints that part of the steering column can separate and cause loss of steering control. No crashes or injuries were reported, the National Highway Traffic Safety Administration said in documents posted September 15 on its Web site. Investigators will determine if the cars have a safety defect and whether a recall is needed. So far the vehicles have not been recalled. A Ford spokeswoman said that the company is aware of the investigation and is cooperating. The investigation only affects police versions of the Crown Victoria, she said. The Montgomery County, Maryland, Police Department said earlier the week of September 10 it was inspecting its 324 Crown Victorias because of a steering problem with its cruisers. Police in Tucson, Arizona also recently began inspecting its fleet of Crown Victorias. The police officer union says that at least six vehicles were found to be deficient and in need of repair. Source: http://www.dailyherald.com/article/20120915/business/709159881/

## ENERGY

(Washington) **Everett police investigating remains of small explosive found tied to a power pole.** Everett, Washington police were investigating the remains of a small explosive device found tied to a power pole outside a business September 15, the Everett Herald reported. According to the Herald, someone reported hearing a blast around 8:40 p.m. in the 2400 block of Broadway. Police arrived at the scene to find a small explosive device detonated and tied to a power pole. The device caused very little damage to the pole. Detectives are investigating the explosive and the incident. Source: http://www.q13fox.com/news/kcpq-everett-police-investigating-remains-of-small-explosive-found-tied-to-a-power-pole-20120917,0,3174702.story

**Entergy estimates Hurricane Isaac damage at $500 million.** Entergy Corp said September 18 that damage from Hurricane Isaac would cost its utilities between $400 million and $500 million and would reduce power sales in the third quarter. Entergy, which supplies electricity to 2.8 million customers in Arkansas, Louisiana, Mississippi, and Texas, said Hurricane Isaac left more than 787,000 customers without power and damaged its power delivery infrastructure. Isaac, which struck the Louisiana coast with 80 mph winds August 28, ranks as the fourth worst storm in Entergy's history in terms of power outages. Distribution systems of the utilities had extensive damage, Entergy said. Preliminary estimates showed that Isaac had damaged or destroyed 4,500 poles and 2,000 transformers. The storm also knocked 95 transmission lines

out of service along with 144 substations. No damage has been identified at Entergy's fossil or nuclear power plants, but detailed assessments are continuing, the company said. Entergy Louisiana's repair cost from Isaac is estimated at $240 million to $300 million, followed by Entergy Gulf States Louisiana at $70 million to $90 million; Entergy New Orleans at $50 million to $60 million; Entergy Mississippi at $30 million to $40 million, and Entergy Arkansas at $10 million, according to a company statement. Source: http://www.reuters.com/article/2012/09/18/us-entergy-outlook-idUSBRE88H0NP20120918

(Washington; Idaho) **Wire thieves creep through Idaho, Washington State.** Thieves in northern Idaho and eastern Washington State are still targeting copper wire for the scrap market despite lower metal prices and electrocution risks, power company officials say. Officials tell the Spokane Spokesman-Review that thieves cause higher electricity bills for customers and endanger the public by leaving live wires. The communications manager for Avista Utilities said thieves have cut down live lines and climbed substation fences to steal equipment that could kill them. He said the company recently discovered copper grounding wire, worth about $200 on the scrap metal market, missing from about 60 poles in rural areas north and south of Coeur d'Alene, Idaho. He said it will cost about $10,000 to replace ground wires, with ratepayers paying for the thefts. He also said the missing grounding wire means line crews do not have a safety guard to tie into while working on the poles. And if a storm or car crash knocks down a pole, the wires might not de-energize properly. In addition, voltage fluctuations can be caused by improperly grounded power lines that can damage home electronics. Source: http://seattletimes.com/html/localnews/2019173847_apwawirethieves1stldwritethru.html

## Food and Agriculture

**Cheese maker put on import alert after Listeria outbreak.** The U.S. Food and Drug Administration placed Italian company Fattorie Chiarappa on import alert after the company's product was linked to a multistate Listeria outbreak, reported Food Safety News September 18. All cheese from this company will be barred from entering through ports of entry unless the company can show that it is not contaminated. To date, 14 people in 11 States have contracted Listeria infections thought to be linked to Ricotta Salata Frescolina cheese distributed by Forever Cheese Inc of Long Island City, New York. Whole Foods and one Washington State distributor have recalled the cheese in response to the investigation into the outbreak. Source: http://www.foodsafetynews.com/2012/09/cheese-maker-put-on-import-alert-after-listeria-outbreak/#.UFnOypH2q70

**Canadian ground beef recall extends to U.S.** Some of the ground beef products recalled by a Canadian firm the week of September 17 for possible E. coli contamination were sold to processors in the United States, announced a U.S. distributor September 17. The potentially contaminated ground beef products, manufactured by XL Foods of Alberta, Canada, were tested by the U.S. Department of Agriculture when entering the United States at the Canadian border and were found to contain E. coli O157:H7, according to a press release from US Foods. The affected meat was sold by XL Foods to at least two large U.S. processors, including Morasch Meats of Portland, Oregon, and Cattleman's (a US Foods brand), according to the director of

regulatory compliance at US Foods, which buys ground beef from these processors and distributes it to retail locations. US Foods distributed the XL Foods ground beef from three Pacific-region centers. US Foods said it started to contact customers who purchased products subject to the recall. Source: http://www.foodsafetynews.com/2012/09/canadian-ground-beef-recall-extends-to-us/#.UFnOwZH2q70

## Government Sector (including Schools and Universities)

**Majority of US schools not ready for next pandemic, SLU researchers say.** Many U.S. schools are not prepared for bioterrorism attacks, outbreaks of emerging infectious diseases or pandemics, despite the recent 2009 H1N1 influenza pandemic that resulted in more than 18,000 deaths worldwide, Saint Louis University researchers say. The study surveyed about 2,000 nurses working in elementary, middle, and high schools across 26 States. The findings reveal that only 48 percent of schools address pandemic preparedness and only 40 percent of schools have updated their plans since the 2009 H1N1 pandemic that spread illnesses in more than 214 countries. Published in the American Journal of Infection Control, the study also found that 44 percent of schools do not participate in community surveillance that tracks the presence of a disease based upon symptoms reported by area residents. These efforts are coordinated through local public health departments that assess indicators of biological threats. In order to have a regular and strong pandemic preparedness program, the study's lead researcher suggests that school nurses should be involved in building and assessing the plan. Source: http://slu.edu/x67767.xml

(Louisiana) **Man arrested in Louisiana State University bomb threat case.** A man has been arrested in connection with a bomb threat that led to an evacuation of Louisiana State University September 17, school police said. The man, of Baton Rouge, Louisiana, was arrested September 18 for communicating false information of a planned bombing, police said. The school, located in Baton Rouge, evacuated buildings after authorities received a call saying there were multiple bombs on campus and that they would detonate in 2 hours. Students were allowed back in buildings hours later after authorities searched the campus. LSU has about 29,000 students and 4,700 faculty and staff members. Source: http://www.reuters.com/article/2012/09/19/us-usa-louisana-bomb-idUSBRE88I10220120919

(Louisiana) **Students return to Louisiana State University after bomb scare.** Students at Louisiana State University (LSU) in New Orleans were allowed to return to their dorms late September 17 after police swept residential halls on the campus following a bomb threat. Dining and recreational facilities also were reopened, LSU said in a statement. The university was evacuated following a telephoned threat to the East Baton Rouge Parish emergency center at 10:32 a.m. and the center relayed the information to campus police, said a university spokesman. The university chancellor made the decision to evacuate the campus, and LSU alerted students, faculty, and staff via text message at about 11:30 a.m., he said. As word of the threat spread, public school officials placed three nearby elementary schools and one high

school on lockdown, according to the East Baton Rouge Parish School System. Louisiana State Police were talking to their counterparts in other areas of the nation where university bomb threats were reported the week of September 10 of to determine whether there were similarities. Source: http://www.reuters.com/article/2012/09/18/us-usa-louisiana-evacuation-idUSBRE88G15820120918?feedType=RSS&feedName=domesticNews

(California) **CA man arrested after blog post about killing kids.** A statement issued September 18 by the Los Angeles County sheriff says a man with guns in his Valencia, California home that overlooks two schools wrote an Internet post saying he was watching kids and would not mind murdering them. He was arrested on suspicion of making terrorist threats. The statement said Bristol, Connecticut police alerted sheriff's investigators to the blog, where an anonymous man said he wanted to kill kids like July's shootings in a movie theater in Aurora, Colorado. Investigators linked the posting to the man's home, where several firearms were found. Sheriff's officials are working with Bristol police and Yale University police. Source: http://www.sfgate.com/news/article/CA-man-arrested-after-blog-post-about-killing-kids-3872900.php

## Information Technology and Telecommunications

**Users of mobile portals exposed to HTTP header pollution attacks, expert finds.** At the EUSecWest security conference in Amsterdam, Netherlands, an independent security researcher unveiled his findings on GSM vulnerabilities in a paper entitled —Using HTTP headers pollution for mobile networks attacks. The attacks he demonstrated target the Wireless Application Protocol (WAP) and Web portals on which the customers of mobile operators can perform specific tasks such as money transfers, content downloads, and subscriptions. Depending on the services offered by the carrier on these Web sites, cyber criminals can abuse the security holes for their own gain. Apparently, there is also a way for shady companies to take advantage of these flaws. Third-party mobile content providers can enter agreements with the carrier and secretly subscribe customers to their paid services. A majority of the sites tested by the researcher — belonging to operators from all over the world — were found to be vulnerable to the attack method he identified. Source: http://news.softpedia.com/news/Users-of-Mobile-Portals-Exposed-to-HTTP-Header-Pollution-Attacks-Expert-Finds-293540.shtml

**Over 1 million PCs currently part of ZeroAccess global botnet.** The piece of malware known as ZeroAccess is present on more than 1 million computers spread throughout almost 200 countries. So far, the threat was found to be installed more than 9 million times on the devices of unsuspecting users. The total number of installs reached this limit in just several months. ZeroAccess generates a profit for its masters with the aid of a peer-to-peer network that is used to download malicious plugins. These components are capable of carrying out diverse tasks that help the criminals make money. According to experts, cyber criminals can earn as much as $100,000 per day if the botnet is operating at maximum capacity. After monitoring the threat for 2 months, Sophos was able to pinpoint the locations of the infected machines. Most appear to be in the United States (55 percent), Canada, the United Kingdom, Germany, Turkey, Spain,

France, Austria, Italy, and Japan. Source: http://news.softpedia.com/news/Over-1-Million-PCs-Currently-Part-of-ZeroAccess-Global-Botnet-293573.shtml

**New NIST publication provides guidance for computer security risk assessments.** The National Institute of Standards and Technology (NIST) released a final version of its risk assessment guidelines which, NIST says, can provide senior leaders and executives with the information they need to understand and make decisions about their organization's current information security risks and information technology infrastructures. A NIST release notes that information technology risks include risk to the organization's operations (including, for example, missions and reputation), its critical assets such as data and physical property, and individuals who are part of or served by the organization. In some cases, these risks extend to the nation as a whole. Risk assessments are part of an organization's total risk management process. Source: http://www.homelandsecuritynewswire.com/dr20120920-new-nist-publication-provides-guidance-for-computer-security-risk-assessments

**Victims of phishing attacks unaware their websites are compromised, APWG finds.** A study by the Anti-Phishing Working Group (APWG) reveals many Web site owners whose domains have been compromised by phishers are unaware that they are victims of a cybercriminal operation. In order to ensure their phishing campaigns do not get interrupted by security solutions providers, cybercriminals often take over legitimate hosts on which they plant their malicious Web pages. The results of the study show attackers are still mostly targeting environments that rely on Linux, Apache, MySQL, andPHP. The biggest concern is that in 80 percent of the cases, the site's owners are unaware they are part of a criminal operation until a third party notifies them. In 40 percent of cases, phishing pages are removed from sites within 24 hours after they were planted. Close to 60 percent of the respondents claimed to have taken down the malicious Web sites within 2-3 days. Most individuals who experienced such incidents do not know much about how they became victims. Source: http://news.softpedia.com/news/Victims-of-Phishing-Attacks-Unaware-Their-Websites-Are-Compromised-APWG-Finds-293391.shtml

**New iteration of TDSS/TDL-4 botnet uses domain fluxing to avoid detection.** A new version of the TDSS/TDL-4 botnet is rapidly growing, primarily because it is having success using an evasion technique known as a domain generation algorithm (DGA) to avoid detection, researchers at Damballa Security revealed September 17. The algorithm helps the latest version of the botnet conduct click-fraud campaigns and is used primarily to rapidly move communication between victims and command-and-control servers from domain to domain, a technique known as domain fluxing, similar to fast fluxing. Since this new version appeared in May, it has reportedly infected 250,000 unique victims, including machines inside government agencies, ISP networks, and 46 of the Fortune 500. Damballa researchers said they found 85 command and control servers and 418 domains related to the new version, primarily hosted in Russia, Romania, and the Netherlands. Source: http://threatpost.com/en_us/blogs/new-iteration-tdsstdl-4-botnet-uses-domain-fluxing-avoid-detection-091712

**Microsoft confirms hackers exploiting critical IE bug, promises patch.** September 17, Microsoft issued a security advisory that confirmed in-the-wild attacks are exploiting an unpatched bug in

Internet Explorer (IE). The software maker is working on a fix. The advisory addressed the zero-day vulnerability that was found and disclosed by a researcher the weekend of September 15. September 17, the Metasploit open-source penetration framework published an exploit module for the bug. All but one supported edition of IE are affected: 2001's IE6, 2006's IE7, 2009's IE8, and 2011's IE9. Together, those browsers accounted for 53 percent of all browsers used worldwide in August. The only exception was IE10, the browser bundled with the new Windows 8, which does not contain the bug. Microsoft acknowledged it was investigating reports of a vulnerability but it did not promise a patch. The bug, when Microsoft patches it, will be rated —critical. Exploiting the flaw allows hackers to execute code and opens Windows XP, Vista, and Windows 7 to drive-by attacks that only require getting victims to visit a malicious or compromised Web site. Until a patch is available, Microsoft recommends users block attacks with EMET 3.0 (Exploit Mitigation Experience Toolkit), boost IE's security zone settings to —high, and configure the browser to display a warning before executing scripts. Source: http://www.computerworld.com/s/article/9231396/Microsoft_confirms_hackers_exploiting_critical_IE_bug_promises_patch

**Your PC may come with malware pre-installed.** Microsoft researchers investigating counterfeit software in China found that new systems being booted for the first time were already compromised with botnet malware right out of the box. Microsoft filed a computer fraud suit against a Web domain registered to a Chinese businessman. The suit alleges the Nitol malware on the new PCs points the compromised systems to 3322.org. Microsoft believes the site is a major hub of malware and malicious online activity. Microsoft claimed that the site in question hosts Nitol, as well as 500 other types of malware. A Washington Post report stated it is the largest single repository of malicious software ever encountered by Microsoft. Source: http://www.pcworld.com/article/262325/your_pc_may_come_with_malware_pre_installed.html

**Tool scans for RTF files spreading malware in targeted attacks.** Exploits embedded inside Microsoft Office documents such as Word, PDFs, and Excel spreadsheets have been at the core of many targeted attacks during the past 2 years. Detection of these attack methods is improving and hackers are recognizing the need for new avenues into enterprise networks. Some have been finding success using rich text format (RTF) files to spread malware that exploits Office vulnerabilities. In June, a researcher reported she collected 90 RTF files over the course of 3 months, many with China-related file names and many targeting specific industries. All of them were exploiting CVE-2012-0158, a vulnerability in Active X controls within MSCOMCTL.OCX—OLE files developed by Microsoft to allow object linking and embedding to documents and other files. Source: http://threatpost.com/en_us/blogs/tool-scans-rtf-files-spreading-malware-targeted-attacks-091412

**Stolen iOS data used as malware lure.** The recent high-profile breach of Apple iOS device data has become the latest lure for malware writers looking to infect users. Researchers with McAfee discovered a series of files being advertised on download services as an archive of the data stolen by hackers affiliated with the Anonymous AntiSec campaign. Though the hackers

claimed the data was lifted from the personal laptop of an FBI agent, the bureau denied the claim and a U.S. publisher later took the blame for the breach. According to a McAfee senior threat researcher, the attackers hid a trojan as a file made to look as if it contained the hacked data. —As you might have guessed, this file is not the real list but an _exe' file and, of course, a malware, he said. —[W]e recommend you take care before downloading an alleged sensational file. Source: http://www.v3.co.uk/v3-uk/news/2205805/stolen-ios-data-used-as-malware-lure

## National Monuments and Icons

Nothing Significant to Report

## Postal and Shipping

(Washington) **4 postal service employees mysteriously fall ill in Lake Stevens.** More than 30 postal service employees were examined by paramedics September 18 at a U.S. Postal Service Annex in Lake Stevens, Washington, after several workers fell ill. Four workers were taken to a hospital for evaluation after complaining of feeling sick. The annex was evacuated. Crews trained in handling hazardous materials were called to search the building, but nothing was found. The sick employees showed symptoms of nausea and weakness. Since the initial incident there were no other complaints. Crews are still working to determine the source of the sickness. Source: http://www.q13fox.com/news/kcpq-4-lake-stevens-postal-service-employees-fall-ill-20120918,0,1470476.story

(Utah) **Police: Man took hostage in office building.** Police are investigating why a knife-wielding man took a worker hostage in the elevator of a downtown Salt Lake City building that houses FBI offices September 17. Salt Lake City police say the man was moving from floor to floor in the building and holding a man against his will at knife-point. He was detained by agents as he stepped off the elevator into the lobby of the FBI offices on the 12th floor. The victim, who works in the building, was unharmed. The Salt Lake Tribune reports the man did not resist arrest and was booked on suspicion of aggravated kidnapping. KTVX 4 Salt Lake City reports police have not determined a motive for the hostage taking or whether it was targeted to the FBI. Source: http://www.sfgate.com/news/article/Police-Man-took-hostage-in-office-building-3874064.php

## Public Health

(Maryland) **NIH superbug claims 7th victim.** A deadly, drug-resistant superbug outbreak that began during the 2011 summer at the National Institutes of Health Clinical Center claimed its seventh victim September 7, when a seriously ill boy from Minnesota succumbed to a bloodstream infection, officials said September 14. The boy was the 19th patient at the research hospital to contract an antibiotic-resistant strain of the bacterium Klebsiella pneumoniae that arrived in August 2011 with a New York woman who needed a lung transplant. But his case marked the first new infection of this superbug at NIH since January —

a worrisome signal that the bug persists inside the huge brick-and-glass federal facility in Bethesda, Maryland. Source: http://www.washingtonpost.com/national/health-science/nih-superbug-claims-7th-victim/2012/09/14/09b3742e-fe9b-11e1-b153-218509a954e1_story.html

## Transportation

**NTSB issues 2 urgent safety recommendations to FAA.** The National Transportation Safety Board (NTSB) September 18 issued two urgent safety recommendations to the Federal Aviation Administration (FAA) regarding two recent occurrences in which the fan midshaft on General Electric GEnx-1B engines fractured or exhibited crack indications; and a GEnx -2B incident that appears similar in nature. The recommendations are: (1) Issue an airworthiness directive to require, before further flight, the immediate ultrasonic inspection of the fan midshaft in all GEnx-1B and -2B engines that have not undergone inspection, and (2) Require repetitive inspections of the fan midshaft at a sufficiently short interval that would permit multiple inspections and detection of a crack before it could reach critical length and the fan midshaft fractures. July 28 the NTSB initiated an investigation of an engine failure that occurred on a Boeing 787 during a pre-delivery taxi test in Charleston, South Carolina. This investigation is ongoing. In addition, August 31, a GEnx-1B engine installed on a Boeing 787 that had not yet flown was found to have an indication of a similar crack on the fan midshaft. The fan midshaft was removed from the engine for further inspection and examination. As a result of the investigative work to date, the NTSB has determined that the fan midshafts on the GEnx engines fractured or cracked at the forward end of the shaft where the retaining nut is installed. Source: http://news.thomasnet.com/companystory/NTSB-Issues-2-Urgent-Safety-Recommendations-to-FAA-621970

## Water and Dams

(Utah) **Cedar Hills residents get giardia parasite from dirty water supply.** Since early July, residents in a Cedar Hills, Utah, neighborhood, kept getting sick, with symptoms worsening by September, KSL 5 Salt Lake City reported September 16. Several residents were diagnosed with giardia, a parasite that can be found in water, uncooked food, excrement, and soil. The only common factor among the 13 affected houses was dirty yellow water. The area had been receiving water from Manila Water Company until that company went bankrupt earlier in the summer. July 5, a private contractor moved its line to an existing Cedar Hills system, the same time residents began falling ill. —We did find a cross-connect in (a) cluster of valves where there was a 2-inch lateral tied from the culinary irrigation to the pressurized irrigation, said the city manager. A small, unknown pipe was allowing in secondary water but the city was unaware and it was never identified on the construction plan. That pipe has since been patched and the city flushed the system with chlorine and fresh water. It will be testing the water through September 21 to make sure the giardia is contained. A notice asking residents to boil their water to kill off the germ was expected to be lifted within a week. Source: http://www.ksl.com/?nid=148&sid=22177222

# Homeland Security Contacts

**To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

**To contribute to this summary or if you have questions or comments, please contact:**

**Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168**